الخليج

اقتصاد, تقنية وسيارات

19 سبتمبر 2022 16:56 مساء

ريد لاين» برمجية خبيثة تنتشر ذاتياً لسرقة بيانات اللاعبين على اليوتيوب»

دبي:

«الخليج»

كشف باحثو كاسبرسكي حزمة برمجية خبيثة غير اعتيادية، وهي عبارة عن مجموعة من برمجيات خبيثة موزعة على شكل ملف للتثبيت، أو أرشيف يتم استخلاصه ذاتياً، أو تكون على شكل ملف من نوع آخر يشتمل على وظائف تشبه «البرامج القابلة للتثبيت. وتستهدف اللاعبين على اليوتيوب، حيث تتكون حمولتها الرئيسية من برمجية «ريد لاين المنتشرة على نطاق واسع، كما تعدّ أحد أكثر البرمجيات شيوعاً، والتي تستخدم أساساً لسرقة كلمات RedLine المرور وبيانات الاعتماد من المتصفحات.

وينشط مجرمو الإنترنت في البحث عن حسابات الألعاب وموارد الألعاب الإلكترونية، حيث لاحظ خبراء كاسبرسكي في آخر تقرير حول التهديدات الإلكترونية ذات الصلة بالألعاب، أن البرامج الخبيثة لغرض السرقة غالباً ما يتم توزيعها تحت ستار اختراق الألعاب والغش وكسر حواجز الحماية. وفي هذه المرة، تم اكتشاف نوع آخر من الأنشطة الخبيثة في عالم الألعاب، وتمثلت في قيام المهاجمين بوضع نوع من الحزم المسمومة داخل قنوات الضحايا على اليوتيوب، يتم استخراجه ذاتياً في وصف RAR والتخفّي تحت ستار المحتوى المرتبط بالألعاب، مع رابط لأرشيف الملفات بنسق

الفيديو. ويحتوي الأرشيف ذاته على العديد من الملفات الخبيثة، ومن بينها برمجية السرقة «ريد لاين».
وتمتلك هذه البرمجية القدرة على سرقة أسماء المستخدمين وكلمات المرور وملفات تعريف الارتباط، إضافة إلى «و «جيكو Chromium «تفاصيل البطاقة المصرفية، والبيانات التي تتم تعبئتها تلقائياً من المتصفّحيْن «كروميوم كما أنها VPN / SSH / FTP وبيانات محافظ العملات المشفرة وبرامج المراسلة الفورية وبرامج العملاء Gecko تطال الملفات ذات الامتدادات الخاصة من الأجهزة. وعلاوة على كل ما ذكر، تستطيع هذه البرمجية الخبيثة تنزيل وفتح الروابط في المتصفح cmd.exe برامج الجهات الخارجية وتشغيلها، والملف التنفيذي لتوجيه الأوامر الأوامر الافتراضي، كما لوحظ قدرتها على الانتشار بطرق مختلفة، بما في ذلك رسائل البريد الإلكتروني الخبيثة، وبرامج التحميل التابعة لجهات خارجية.
وفضلاً عن وجود برمجية «ريد لاين» ضمن حمولة الحزمة، تمتاز الحزمة المكتشفة ذاتها بقدرتها على الانتشار الذاتي، كما أنها تشتمل على العديد من الملفات المسؤولة عن هذه المهمة، ناهيك عن استقبال مقاطع فيديو ونشرها على قنوات اليوتيوب للمستخدمين المتضررين، مع وصولها إلى روابط الأرشيف المحمي بكلمة المرور. وتعلن مقاطع الفيديو عن :عمليات الغش والاختراق، كما تقدم الإرشادات حول سبل اختراق الألعاب والبرامج الشائعة. ومن بين هذه الألعاب Farthest و Farming Simulator و F1 22 و Dying Light 2 و DayZ و CrossFire و APB Reloaded و Point Blank و Osu و Lego Star Wars و Forza و Final Fantasy XIV و FIFA 22 و Frontier .Walken و VRChat و Thymesia و Stray و Spider-Man و Sniper Elite و Rust و Project Zomboid

نماذج من مقاطع الفيديو التي تنشر الحزمة

ذاتياً، كما تحتوي RAR وحال قيام الضحايا بتنزيل الحزمة الأصلية بأنفسهم، يتم استخلاص أرشيف الملفات بنسق الحزمة على عدد من الملفات الخبيثة والأدوات المساعدة النظيفة، مع وجود برنامج نصّي يتمثل دوره في تشغيل .المحتويات غير المضغوطة تلقائياً، بينما تتضمن بعض أسماء الملفات لغة صريحة

محتويات أرشيف الاستخلاص الذاتي

ومن بين العناصر الأخرى التي لفتت انتباه الباحثين، وجودة أداة التعدين التي تأتي من منطلق افتراض أن اللاعبين باعتبارهم الجمهور المستهدف الرئيسي، يقومون بتقييم الفيديو، ويحتمل قيامهم بتثبيت بطاقات فيديو لاستخدامها في أغراض التعدين.
وقال أوليغ كوبريف، كبير الباحثين الأمنيين في كاسبرسكي: «يعتبر اللاعبون من أكثر الفئات المستهدفة من قبل مجرمي الإنترنت. واستخدم المهاجمون هذه المرة المحتوى المرتبط بالألعاب التي يتخذونها طُعماً لسرقة بيانات اعتماد الضحايا وأنشطة التعدين من أجهزتهم الحاسوبية. وهنا نتوجه بالنصيحة إلى هذه الفئة تحديداً بضرورة اختيار .«المصادر بعناية، بما يتناسب مع الألعاب، وعدم تنزيل أي أرشيفات مشبوهة من حسابات غير موثوقة